

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

GIULIO MECOCCI,

Plaintiff,

v.

YOUNG CONSULTING, LLC,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Giulio Mecocci (“Plaintiff”), on behalf of himself and all others similarly situated, alleges the following against Defendant Young Consulting, LLC (“Defendant”) upon personal knowledge as to his own acts, and based upon his investigation, his counsel’s investigation, and information and belief as to all other matters.

INTRODUCTION

1. This is a Data Breach class action against Defendant Young Consulting, LLC (“Young Consulting”) on behalf of individuals whose personally identifying information (“PII”) and personal health information (“PHI”) was stolen and released by a ransomware gang who breached Defendant’s systems at least as early as April 2024.

2. Defendant Young Consulting is a risk management company, which services Blue Shield of California (“Blue Shield”). As part of its risk management services, Defendant collects, stores, and maintains significant PII and PHI for at least hundreds of thousands of Blue Shield’s individual subscribers.

3. On August 26, 2024, Young Consulting announced that its systems had been breached by a ransomware gang and that information on at least 954,177 subscribers had been compromised. The breach itself occurred at least as early as April 10, 2024, and Defendant stated it became aware of the breach on April 13, 2024.

4. According to news reports, the cyberattack was carried out by the “BlackSuit” ransomware gang, who claimed responsibility for the attack as early as May 7, 2024. It began releasing leaked sensitive information a few weeks later.¹

5. The information breached includes at least the subscriber’s full name, Social Security number, date of birth, and private medical insurance claim information.

6. Although this information is not confirmed, “BlackSuit” claimed to leak a lot more than what Young Consulting disclosed on the notices to impacted individuals. Specifically, BlackSuit claimed the breached information also included

¹ <https://www.bleepingcomputer.com/news/security/blacksuit-ransomware-stole-data-of-950-000-from-software-vendor/> (Last Accessed September 6, 2024)

contracts, presentations, employee passports, contacts, family details, medical examinations, financial audits, reports and payments, and various content taken from personal folders and network shares.²

7. Even after this sensitive information was released, Defendant did not even notify Blue Shield until June 28, 2024, nearly a month later.³ Defendant then further, inexplicably, delayed an additional two months before notifying individuals who were impacted in the breach starting on August 26, 2024.

8. Defendant is a risk management company and understands the extremely the high value of this information, including medical information, to outside parties including criminal organizations. Defendant knew or should have known about the risk to the data they stored and processed, and the critical importance of adequate security measures in the face of increasing threats.

9. Despite knowing the risks, Defendant did not implement adequate security measures to protect subscribers' PHI and PII.

10. The failure to implement adequate data security measures in the face of the obvious threat profile made a data breach entirely foreseeable, and indeed probable. But for Defendant's failure to secure and encrypt their production servers and appropriately isolate and compartmentalize data on their patients, this breach

² *Id.*

³ <https://youngconsulting.com/notice/youngconsulting-notice.html> (last accessed September 6, 2024).

would not have occurred.

11. Plaintiff and the Class have been harmed because they are at immediate risk of having their personal information used against them, including by means of fraud and identity theft. Indeed, they have been at risk well before Defendant even notified Plaintiff of the breach. Plaintiff also suffered harm in the loss of his private medical and personal information and the extreme risk of sale of this data to criminals over the dark web, which may have already occurred.

12. Under these circumstances, Defendant unreasonably delayed notifying individual victims of the specific information that was breached, including for months after it was leaked online to criminal actors. As of September 8, 2024, Defendant has still not identified precisely what information was breached in the attack. This delay in notification to victims of the breach is unacceptable and directly harms victims of the breach, including Plaintiff, by creating uncertainty about the extent to which they have been harmed and the need to engage in various services and efforts in the wake of the data breach, including but not limited to examining whether their PII or PHI has been sold on the dark web, taking measures to protect against identity theft crimes, spending money and/or time on credit monitoring and identity theft insurance, examining bank statements, initiating fraud alerts, and other efforts at mitigating consequential harms.

13. Plaintiff, individually and on behalf of a nationwide class, alleges claims of (1) Negligence and Negligence *Per Se*, (2) Breach of Implied Contract, and (3) Unjust Enrichment. Plaintiff also seeks declaratory and injunctive relief. Plaintiff asks the Court to compel Defendant to adopt reasonable information security practices to secure the sensitive PII and PHI that Defendant collects and stores in its databases and to grant such other relief as the Court deems just and proper.

PARTIES

Plaintiff

14. Plaintiff Giulio Mecocci is a resident of Jersey City, New Jersey. He was a subscriber to Blue Shield of California and received a data breach letter from Young Consulting dated August 26, 2024.

Defendant

15. Defendant Young Consulting, LLC advertises itself as “the market leader in providing software solutions to the employer stop loss marketplace.”⁴ It is a risk management company organized under the laws of Georgia. Defendant’s principal place of business registered with Georgia’s Secretary of State is 1 E Wacker Drive, STE 2900, Chicago, IL, 60610. Defendant’s websites identify their

⁴ <https://www.youngconsulting.com/> (last accessed September 6, 2024).

location as Atlanta, Georgia.⁵

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction and diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The class contains more than 100 members (indeed, it likely contains nearly one million members), and many of these members have citizenship diverse from Defendant.

17. Upon information and belief, at least one member of the proposed class is diverse from at least one member of Defendant.

18. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the case in controversy.

19. The exercise of personal jurisdiction over Defendant is appropriate because Young Consulting, LLC is a Georgia Limited Liability Company, regularly transacts business in this District, listed a principal office in Georgia with the Secretary of State's Office until earlier this year, continues to be located in Georgia according to its websites, and sent out data breach notification letters listing an address in Georgia: 3200 Windy Hill Road SE, Suite 1400W, Atlanta, GA 30339.

20. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the

⁵ *Id.*; <https://connexure.co/about-us/> (last accessed Sept. 9, 2024).

claims emanated from activities within this District. Specifically, Young Consulting is organized in Georgia and its breached systems, representations, decision making, and security practices emanated from this District.

FACTUAL ALLEGATIONS

I. Background

21. Defendant is a company which offers risk management technologies, analysis, and software to insurance companies such as Blue Shield of California.

22. Plaintiff and members of the Plaintiff Class are former or current insured individuals whose insurance company, most notably Blue Shield of California, who provided their PII and PHI to their insurance company as a prerequisite for receiving healthcare services.

23. In order to receive treatment, Plaintiff and members of the Plaintiff Class were required to provide all or part of the following non-exclusive list of sensitive PHI and PII during the regular course of business:

- Full name and mailing or personal address,
- State and/or Federal Identification,
- Social Security Number,
- Health insurance information including but not limited to carrier, policy number, and healthcare card,
- Date of birth,

- Medical information including but not limited to information about diagnosis and treatment, personal medical history, family medical history, mental health information, information related to STDs and treatment, medication information, and medical record number,
- Information about physicians and related medical professionals who had been involved in previous or ongoing treatment of the patient,
- Residence and travel history,
- Billing and claims information including but not limited to information related to credit and debit card numbers, bank account statements and account numbers, and insurance payment details,
- Medicare/Medicaid information,
- Information on prescriptions taken including history of taking certain prescriptions,
- Diagnostic results and treatment information,
- Information on family members including but not limited to emergency contact information and next of kin,
- Personal email addresses and phone numbers, and/or
- Workers' compensation and employment information.

24. The above information is extremely sensitive personal identifying information (PII) and personal health information (PHI). This information is

extremely valuable to criminals because it can be used to commit serious identity theft and medical identity theft crimes.

25. Some or all of this extremely sensitive information was subsequently provided by the insurance company to Young Consulting, including the subscriber's full name, Social Security number, date of birth, and private medical insurance claim information.

26. Young Consulting represents on its website privacy policy that it will not provide a subscriber's name without a subscriber's consent.⁶

II. The Breach

27. At least as early as April 10, 2024, Young Consulting suffered a massive breach of its systems. It became aware of this breach at least as early as April 13, 2024.

28. On information and belief, Young Consulting became aware of the breach on April 13, 2024 because its systems were encrypted through a ransomware attack, and the hackers notified Young Consulting that they would begin releasing seized information, including the PII and PHI identified above, unless Defendant paid it a ransom.

29. According to reports, Young Consulting did not pay the ransom.

⁶ <https://www.youngconsulting.com/privacy-policy/> (last accessed September 9, 2024).

Subsequently, subscriber data was leaked by the criminal actors starting in May 2024.

30. The data breach impacted nearly one million subscribers. At minimum, the breached data included the subscriber's full name, social security number, date of birth, and private medical insurance claim information (which would seem to include medical information including on submitted healthcare claims, treatments, costs, and more). Young Consulting's opaque use of the term "insurance policy/claim information" in its data breach letter does little to clarify the scope or scale of the breached information.

31. On June 28, 2024, Young consulting notified Blue Shield California of the breach. This is more than two months after the breach occurred and at least one month after subscriber data was leaked online in May.

32. On August 26, 2024, Young Consulting finally started the process of notifying individual subscribers whose data was compromised in the breach. This is more than four months after Young Consulting first became aware of the data breach.

33. Young Consulting as of September 6, 2024 has not disclosed the precise cause of the data breach, the efforts, if any, Young Consulting has taken to mitigate the harm to subscribers and limit the spread of the leaked data, or offered

any remedy for impacted subscribers beyond offering 12 months of credit monitoring in some instances.

III. Defendant Failed to Comply with Reasonable Cybersecurity Standards

34. At all times relevant to this Complaint, Defendant knew or should have known the significance and necessity of safeguarding its subscribers' PII and PHI, and the foreseeable consequences of a data breach. Defendant knew or should have known that because it collected and maintained the PII and PHI for a significant number of customers, a significant number of customers would be harmed by a breach of its systems. Defendant further knew due to the nature of its business practices as a risk management services provider that the data it was entrusted with was highly valuable and contained private and sensitive information. It further knew that due to it providing services to massive insurance providers, such as Blue Shield, that a data breach could potentially result in the release of deeply personal, sensitive, and costly information about hundreds of thousands of subscribers.

35. Because PII is so sensitive and cyberattacks have become a rising threat, the FTC has issued numerous guides for businesses holding sensitive PII and emphasized the importance of adequate data security practices. The FTC also stresses that appropriately safeguarding PII held by businesses should be factored into all business-related decision making.

36. An FTC Publication titled “Protecting Personal Information: A Guide for Business” lays out fundamental data security principles and standard practices that businesses should implement to protect PII.⁷ The guidelines highlight that businesses should (a) protect the personal customer information they collect and store; (b) properly dispose of personal information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network’s vulnerabilities; and (e) implement policies to correct security problems.

37. The FTC also recommends businesses use an intrusion detection system, monitor all incoming traffic to the networks for unusual activity, monitor for large amounts of data being transmitted from their systems, and have a response plan prepared in the event of a breach.

38. The FTC also recommends that businesses limit access to sensitive PII, require complex passwords to be used on the networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

39. Businesses that do not comply with the basic protection of sensitive PII are facing enforcement actions brought by the FTC. Failure to employ reasonable and appropriate measures to protect against unauthorized access to

⁷ <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last accessed Sept. 9, 2024).

confidential consumer data is an unfair act or practice prohibited pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

40. Many states' unfair and deceptive trade practices statutes are similar to the FTC Act, and many states adopt the FTC's interpretations of what constitutes an unfair or deceptive trade practice.

41. Defendant knew or should have known of its obligation to implement appropriate measures to protect its customers' PII but failed to comply with the FTC's basic guidelines and other industry best practices, including the minimum standards set by the National Institute of Standards and Technology Cybersecurity Framework Version 1.1.⁸

42. Defendant's failure to employ reasonable measures to adequately safeguard against unauthorized access to PII constitutes an unfair act or practice as prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, as well as by state statutory analogs.

43. Defendant failed to use reasonable care in maintaining the privacy and security of Plaintiff' and Class Members' PII and PHI. If Defendant had implemented adequate security measures, cybercriminals could never have accessed the PII of Plaintiff and Class Members, and the Data Breach would have

⁸ <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf> (last accessed Sept. 9, 2024).

either been prevented in its entirety or have been much smaller in scope. For example, if Defendant had implemented adequate monitoring systems, they could have noticed and halted the hacking attempt on April 10, rather than only discover it after the ransomware gang had already seized data and locked down Defendant's systems on April 13. Under normal circumstances no individual should be able to download even a tiny fraction of that information from the subscriber database and adequate monitoring should have flagged and stopped the exfiltrated data much earlier.

44. Moreover, a huge number of systems were compromised by the data breach. The number of compromised systems and the length of time it has taken to bring them back online suggests a fundamental security failure, including a failure to compartmentalize and secure access in the event of a breach. No one individual should ever be able to access all these systems. A reasonable cyber security system would not be able to be so fundamentally deficient. Finally, once Defendant became aware of the breach, they could have acted far faster and more aggressively in responding to the breach and in assisting victims in redressing harms, including sending notifications to those impacted of exactly what data was taken.

45. Personally Identifiable Information is of high value to criminals. Sensitive information can often be sold on the dark web, with personal information being sold at a price ranging from \$40 to \$200 and bank details with a price from

\$50 to \$200.⁹ The Data Breach exposed PII that is both valuable and highly coveted on underground markets because it can be used to commit identity theft and financial fraud. Identity thieves use such PII to, among other things, gain access to bank accounts, social media accounts, and credit cards. Identity thieves can also use this PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government identification cards, or create "synthetic identities." Additionally, identity thieves often wait significant amounts of time—months or even years—to use the PII obtained in data breaches because victims often become less vigilant in monitoring their accounts as time passes, therefore making the PII easier to use without detection. Yet as of March 25, 2024, Defendant has failed even to offer free identity protection services for its customers. Given the extraordinary scale of the breach and the potential for consequences lingering for years. These identity thieves will also re-use stolen PII and PHI, resulting in victims of one data breach suffering the effects of several cybercrimes from one instance of unauthorized access to their PII and PHI.

⁹ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed September 6, 2024).

46. Victims of data breaches are much more likely to become victims of identity fraud. Data Breach victims who do experience identity theft often spend hundreds of hours fixing the damage caused by identity thieves.¹⁰ Plaintiff and members of the Class generally have spent hours on end and considerable time and stress attempting to mitigate the present and future harms caused by the breach. The U.S. Department of Justice’s Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims “reported spending an average of about 7 hours clearing up the issues.”¹¹

47. The information compromised in the Data Breach—including detailed medical information—is much more valuable than the loss of credit card information in a retailer data breach. There, victims can simply close their credit and debit card accounts and potentially even rely on automatic fraud protection offered by their banks. Here, however, the information compromised is much more difficult, if not impossible, for consumers to re-secure after being stolen because it goes to the core of their identity. An individual’s medical history and assessments are permanent and are impossible to escape. The loss of all this medical data puts Defendant customers and patients at additional risk for potential medical fraud and medical identity theft.

¹⁰<https://www.marylandattorneygeneral.gov/ID%20Theft%20Documents/Identitytheft.pdf> (last accessed September 6, 2024).

¹¹<https://bjs.ojp.gov/content/pub/pdf/vit14.pdf> (last accessed September 6, 2024).

48. Data breaches involving medical records are not only incredibly costly, they can “also [be] more difficult to detect, taking almost twice as long as normal identity theft.”¹² The FTC warns that a thief may use private medical information to, among other things, “see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care”¹³ and that this may have far reaching consequences for a victim’s ability to access medical care and use insurance benefits.

49. Security standards for businesses storing PII and PHI commonly include, but are not limited to:

- a. Maintaining a secure firewall;
- b. Monitoring for suspicious or unusual traffic on the website;
- c. Looking for trends in user activity including for unknown or suspicious users;
- d. Looking at server requests for PII;
- e. Looking for server requests from VPNs and Tor exit nodes;
- f. Requiring Multi-factor authentication before permitting new IP addresses to access user accounts and PII; and

¹² See *What to Know About Medical Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last visited Sept. 9, 2024).

¹³ *Id.*

- g. Structuring a system including design and control to limit user access as necessary including a user's access to the account data and PII of other users.

50. Defendant styles itself as “the market leader in providing software solutions to the employer stop loss marketplace”. Given Defendant's representations of expertise, Defendant should have been expected to provide adequate security commensurate with the value of the data it utilized. Defendant had an obligation to provide superior security in light of the sensitivity of the information they administered. Defendant failed.

IV. Plaintiff's and Class Members' Experiences

51. To use Defendant's Service, Plaintiff provided sensitive PII and PHI including his full name, address, date of birth, Social Security number, medical records, insurance information, billing, banking, and credit card information, family medical history, and more. Although Defendant has not clarified specifically what information was compromised beyond name, Social Security number, date of birth, and the omnibus “insurance claims information” catch-all, the granularity of the breached data appears to be extremely high. The insurance information referenced may include but not be limited to: patient name and contact information including mail address, email address, and phone number; state and/or federal identification; health insurance information including healthcare cards; medical information

including information related to medical history, diagnosis, and treatment; information about treating physicians and medical professionals; billing and claims information including payment details; medication and prescription history; mental health information, contact information for family members including full names, personal relationship, and phone number; Medicare/Medicaid information; workers comp or employment related information; and more.

52. Plaintiff has taken reasonable steps to maintain the confidentiality of his PII and PHI. When Defendant accepted its duty to store and analyze data from the healthcare companies it did so with the implicit understanding it would be required to use its experience and sophistication to keep this information secure and confidential.

53. As a result of the data breach, Plaintiff was forced to take measures to mitigate the harm, including spending time monitoring credit and financial accounts, researching the Data Breach, and researching and taking steps to prevent and mitigate the likelihood of identity theft.

54. As a result of the Data Breach, Plaintiff suffered actual injuries including; (a) damages to and diminution in the value of Plaintiff's PII and PHI property that Plaintiff entrusted to Defendant as a condition of receiving their services; (b) loss and invasion of Plaintiff's privacy; (c) injuries arising from the

increased risk of fraud and identity theft, including the cost of taking reasonable identity theft protection measures, which will continue for years, among others.

CLASS ACTION ALLEGATIONS

55. Plaintiff brings this action as a class action pursuant to Rules 23(a) and 23(b)(1)-(3) of the Federal Rules of Civil Procedure, on behalf of themselves and a Nationwide Class defined as follows:

All persons in the United States whose PII/PHI were compromised by the Data Breach announced by Young Consulting in August 2024.

56. Excluded from the Nationwide Class are governmental entities, Defendant, any entity in which Defendant have a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

57. This action is brought and may be properly maintained as a class action pursuant to Rule 23. This action satisfies the requirements of Rule 23, including numerosity, commonality, typicality, adequacy, predominance, and superiority.

58. **Numerosity.** The Nationwide Class is so numerous that the individual joinder of all members is impracticable. While the exact number of Nationwide Class Members is currently unknown and can only be ascertained through

appropriate discovery, Plaintiff, on information and belief, allege that the Nationwide Class includes at least hundreds of thousands of members based on Defendant's own representation that information from more than 950,000 subscribers was compromised.

59. **Commonality.** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary among Class Members and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

- a. Whether Defendant knew or should have known that their systems were vulnerable to unauthorized access;
- b. Whether Defendant failed to take adequate and reasonable measures to ensure their data systems were protected;
- c. Whether Defendant failed to take available steps to prevent and stop the breach from happening or mitigating the risk of a long-term breach;
- d. Whether Defendant unreasonably delayed in notifying subscribers of the harm they suffered once the suspicious activity was detected;
- e. Whether Defendant owed a legal duty to Plaintiff and Class Members to protect their PII and PHI;

- f. Whether Defendant breached any duty to protect the personal information of Plaintiff and Class Members by failing to exercise due care in protecting their PII and PHI;
- g. Whether Plaintiff and Class Members are entitled to actual, statutory, or other forms of damages and other monetary relief; and
- h. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief or restitution.

60. **Typicality.** Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way.

61. **Adequacy of Representation.** Plaintiff is an adequate class representative because he is a Nationwide Class Member and his interests do not conflict with the Class interests. Plaintiff retained counsel who are competent and experienced in class action and data breach litigation. Plaintiff and his counsel intend to prosecute this action vigorously for the Class's benefit and will fairly and adequately protect their interests.

62. **Predominance and Superiority.** The Nationwide Class can be properly maintained because the above common questions of law and fact predominate over any questions affecting individual Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of

this litigation because individual litigation of each Class member's claim is impracticable. Even if each Class member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

63. **Declaratory and Injunctive Relief.** The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members that would establish incompatible standards of conduct for Defendant. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class Members and impair their interests. Defendant have acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

CLAIMS FOR RELIEF

Count 1

Negligence

On behalf of Plaintiff and the Nationwide Class

64. Plaintiff incorporates by reference and realleges each allegation in paragraphs 1-63 as though fully set forth herein.

65. Plaintiff was required to provide PII and PHI as a precondition for receiving insurance services. Plaintiff and Class Members entrusted their PII and PHI to with the understanding that it would safeguard their PII and PHI.

66. When the insurance company provided information to Defendant, Defendant accepted this same responsibility to safeguard Plaintiff's PII and PHI.

67. Defendant did not take reasonable and appropriate safeguards to protect Plaintiff and Class Members' PII and PHI.

68. Defendant had full knowledge of the sensitivity of the PII and PHI that it stored and the types of harm that Plaintiff and Class Members could and would suffer if that PII and PHI were wrongfully disclosed.

69. Defendant violated its duty to implement and maintain reasonable security procedures and practices. That duty includes, among other things, designing, maintaining, and testing Defendant's information security controls sufficiently rigorously to ensure that PII and PHI in its possession was adequately secured by, for example, encrypting sensitive personal information, installing

effective intrusion detection systems and monitoring mechanisms, using access controls to limit access to sensitive data, and regularly testing for security weaknesses and failures. Defendants further violated their duty by failing to notify patients of the specific breached data in a timely manner and failing to remedy the continuing harm by unreasonably delaying notifying specific victims who were harmed.

70. Defendant's duty of care arose from, among other things,
 - a. Defendant's exclusive ability (and Class Members' inability) to ensure that its systems were sufficient to protect against the foreseeable risk that a data breach could occur;
 - b. Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to adopt reasonable data security measures; and
 - c. Defendant's common law duties to adopt reasonable data security measures to protect customer PII and PHI and to act as a reasonable and prudent person under the same or similar circumstances would act.

71. Defendant's violation of the FTC Act constitutes negligence per se for purposes of establishing the duty and breach elements of Plaintiff's negligence

claim. Those statutes were designed to protect a group to which Plaintiff and the Class belong and to prevent the types of harm that resulted from the Data Breach.

72. Defendant processes sensitive information for hundreds of thousands of subscribers on behalf of major healthcare conglomerates like Blue Shield of California. Defendant had the financial and personnel resources necessary to prevent the Data Breach. Defendant nevertheless failed to adopt reasonable data security measures, in breach of the duties it owed to Plaintiff and Class Members. Moreover, if Defendant lacked the capacity to safeguard this information, it never should have accepted custody over it.

73. Plaintiff and Class Members were the foreseeable victims of Defendant's inadequate data security. Defendant knew that a breach of its systems could and would cause harm to Plaintiff and Class Members.

74. Defendant's conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's conduct included their failure to adequately mitigate harm through negligently failing to inform patients and victims of the breach of the specific information breached for (as of time of writing) more than four months after the purported first discovery of the breach.

75. Defendant knew or should have known of the inherent risks in collecting and storing massive amounts of PII and PHI, the importance of providing

adequate data security for that PII and PHI, and the frequent cyberattacks within the insurance industry, particularly given its specialization in risk management.

76. Defendant, through its actions and inactions, breached its duty owed to Plaintiff and Class Members by failing to exercise reasonable care in safeguarding their PII and PHI while it was in its possession and control. Defendant breached its duty by, among other things, their failure to adopt reasonable data security practices and their failure to adopt reasonable security and notification practices, including monitoring internal systems and sending notifications to affected victims. Defendant failed to timely notice Plaintiff and Class Members of suspicious activities and failed to implement sufficiently stringent security measures.

77. Defendant inadequately safeguarded consumers' PII and PHI in breach of standard industry rules, regulations, and best practices at the time of the Data Breach.

78. But for Defendant's breach of its duty to adequately protect Plaintiff and Class Members' PII and PHI, Plaintiff and Class Members' PII and PHI would not have been stolen.

79. There is a temporal and close causal connection between Defendant's failure to implement adequate data security measures and notification practices, the Data Breach, and the harms suffered by Plaintiff and Class Members.

80. As a result of Defendant's negligence, Plaintiff and Class Members suffered and will continue to suffer the damages alleged herein.

81. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

Count 2
Breach of Implied Contract
On behalf of Plaintiff and the Nationwide Class

82. Plaintiff incorporates by reference and realleges each allegation in paragraphs 1-63 as though fully set forth herein.

83. Plaintiff and Class Members entered into an implied contract with Defendant when Defendant accepted custody of their PII and PHI.

84. As part of these transactions, Defendant agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify them if their PII or PHI was breached or compromised.

85. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with the legal requirements and industry standards. Plaintiff and Class Members believed that Defendant would use part of the monies paid to Defendant under the implied contracts or the monies obtained from the

benefits derived from the PII and PHI they provided to fund proper and reasonable data security practices.

86. Plaintiff and Class Members would not have provided and entrusted their PII and PHI to Defendant or would have paid less for Defendant's products or services in the absence of the implied contract or implied terms between them and Defendant. The safeguarding of the PII and PHI of Plaintiff and Class Members was critical to realize the intent of the parties.

87. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant.

88. Defendant breached their implied contracts with Plaintiff and Class Members to protect their PII and PHI when they (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) disclosed that information to unauthorized third parties and; (3) failed to notify Plaintiff and Class Members of the specific data breached in a reasonably timely manner.

89. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting

in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

90. As a direct and proximate result of the breach, Plaintiff and class members are entitled to relief as set forth herein.

Count 3
Unjust Enrichment
On behalf of Plaintiff and the Nationwide Class

91. Plaintiff incorporates by reference and realleges each allegation in paragraphs 1-63 as though fully set forth herein.

92. This count is brought in the alternative to Plaintiff's breach of implied contract count.

93. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Defendant should have provided adequate data security for Plaintiff and Class Members.

94. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form of their Private Information as a necessary part of their receiving healthcare services. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

95. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

96. Defendant, however, failed to secure Plaintiff and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

97. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiff and Class Members

and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

98. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

99. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

100. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

101. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained Plaintiff and Class

Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

102. Plaintiff and Class Members have no adequate remedy at law.

103. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, medical identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of the Defendant's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

104. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members were underpaid by Defendant.

Count 4
Injunctive/Declaratory Relief
On behalf of Plaintiff and the Nationwide Class

105. Plaintiff incorporates by reference and realleges each allegation in paragraphs 1-63 as though fully set forth herein.

106. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described herein.

107. Defendant owes a duty of care to Plaintiff and Class Members, which required Defendant to adequately monitor and safeguard Plaintiff's and Class Members' PII and PHI.

108. Defendant and its officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess the PII and PHI belonging to Plaintiff and Class Members.

109. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendant are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and the Class continue to suffer injury as a result of the exposure of their PII and PHI and the risk remains that further compromises of their private information will occur in the future.

110. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure the PII and PHI of Plaintiff and the Class within its care, custody, and control under the common law, Section 5 of FTC Act, and HIPAA;
- b. Defendant breached its duty to Plaintiff and the Class by allowing the Data Breach to occur;
- c. Defendant's existing data monitoring measures do not comply with their obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII and PHI of Plaintiff and the Class within Defendant's custody, care, and control; and

- d. Defendant's ongoing breaches of said duties continue to cause harm to Plaintiff and the Class.

111. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect the PII and PHI of Plaintiff and the Class within its custody, care, and control, including the following:

- a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.
- b. Order that, to comply with Defendant's obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:
 - i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems, networks, and servers on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
 - ii. Encrypting and anonymizing the existing PII and PHI within their servers, networks, and systems to the extent practicable,

and purging all such information which is no longer reasonably necessary for Defendant to provide adequate services;

- iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;
- iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;
- v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems, networks, and servers;
- vi. Conducting regular database scanning and security checks; and
- vii. Routinely and continually conducting internal training and education to inform Defendant's internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

112. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If

another data breach or cybersecurity incident occurs, Plaintiff and the Class will not have an adequate remedy at law because monetary relief alone will not compensate Plaintiff and the Class for the serious risks of future harm. Moreover, Plaintiff and the Class are unable to stop using Defendant's services without experiencing undue hardship. Because providing information to Defendant is a precondition for receiving Medicare benefits, Plaintiffs cannot cease providing this information without losing Medicare access. This would be an extreme financial hardship to large portions of the Class.

113. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff and the Class will likely be subjected to substantial, continued identity theft and other related damages and or additional data breaches and exposure if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a preexisting legal obligation to employ such measures.

114. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent or larger data breach or cybersecurity incident, thus preventing future injury to Plaintiff and the Class and other persons whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

- A. That the Court certify this action as a class action and appoint Plaintiff and their counsel to represent the Class;
- B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII and PHI of Plaintiff and the Class by implementing improved security controls;
- C. That the Court award compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;
- D. That the Court award statutory or punitive damages as allowed by law in an amount to be determined at trial;
- E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts, omissions, and practices;
- F. That the Court award to Plaintiff and Class Members the costs and

disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

G. That the Court award pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury trial on all claims so triable.

Dated: September 9, 2024.

Respectfully submitted,

/s/ Kristen Tullos Oliver

Kristen Tullos Oliver

Georgia Bar No. 941093

J. Cameron Tribble

Georgia Bar No. 754759

THE BARNES LAW GROUP, LLC

31 Atlanta Street

Marietta, GA 30060

Tel: 770-227-6375

Fax: 770-227-6373

ktullos@barneslawgroup.com

ctribble@barneslawgroup.com

Amber L. Schubert*

Daniel L.M. Pulgram*

SCHUBERT JONCKHEER & KOLBE LLP

2001 Union St, Ste 200

San Francisco, CA 94123

Tel: 415-788-4220

Fax: 415-788-0161

aschubert@sjk.law

dpulgram@sjk.law

*Pro Hac Vice petition to be filed.

***Counsel for Plaintiff and
the Proposed Classes***